



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/666,596	09/18/2003	Jerry Joe Langin-Hooper		8537

26667 7590 11/13/2007
LINDA FLEWELLEN GOULD
1665 BRIARGATE BLVD. #101
COLORADO SPRINGS, CO 80920

EXAMINER

KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

11/13/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/666,596

Applicant(s)

LANGIN-HOOPER ET AL.

Examiner

Paula W. Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 August 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 08/28/07. The amendment filed on 08/28/07 have been entered and made of record. Therefore, presently pending claims are 1-12.

Response to Arguments

Applicant's arguments filed 08/28/07 have been fully considered but they are not persuasive because of following reasons.

Applicant argued that unlike the pseudo-random numbers created by the Menezes process, the idem-random numbers of the instant invention are not repeated in a cycle by the claimed process. However the applicant does not claim that the idem-random numbers of the instant invention are not repeated in a cycle.

The applicant argued further that Menezes does not teach that using a sequence of prime numbers and applying a mathematical relationship will generate a sequence of output numbers for which the next number in the output sequence cannot be accurately predicted. This is not found persuasive. The combination of Menezes shown below teaches using a sequence of prime numbers and applying a mathematical relationship will generate a sequence of output numbers for which the next number in the output sequence cannot be accurately predicted.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

Art Unit: 2135

According to the applicant, this extraordinary and useful result is achieved by the claimed invention, but not by the processes taught in Menezes. However, the arguments of counsel cannot take the place of evidence in the record. An assertion of what seems to follow from common experience is just attorney argument and not the kind of factual evidence that is required to rebut a prima facie case of obviousness.

The applicant argues further that Menezes does not suggest that there would be any value to using prime or prime-like numbers as input numbers in the course of creating pseudo-random numbers. This is not found persuasive. The system of Menezes discloses further using the key, k , which by definition a good key is a prime number.

The applicant argues that Menezes relies on fairly complex mathematical transformations of simple sequences of numbers to generate pseudo-random numbers, idem numbers can be easily and unpredictably created with relatively simple function applied to sequences of prime or prime-like numbers. As stated above, an assertion of what seems to follow from common experience is just attorney argument and not the kind of factual evidence that is required to rebut a prima facie case of obviousness.

The applicant argues that the claimed invention does not utilize sampling, as disclosed by Menezes. The applicant does not claim this limitation.

Claim Rejections - 35 USC § 101

The arguments referring to the 35 USC 101 are persuasive and therefore the 35 USC 101 rejection is withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over the book by Menezes ("Handbook of Applied Cryptography").

In reference to claims 1, 6, and 11 Menezes teaches software based random number generators that identifies a mathematical relationship to be applied to said initial number and said subsequent numbers (section 5.3 page 173 and part ii section 5.2 page 172); applying said mathematical relationship to said initial number and said subsequent number to generate an idem-random number (section 5.3 page 173).

Menezes teaches further methods for finding prime number that include establishing an initial prime number; establishing a subsequent prime number identification condition; determining a first subsequent prime number satisfying the subsequent prime number identification condition applied to the initial prime number (section 4.4.1 pages 145-146).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the prime number that is generated in Menezes (section 4.4.1 pages 145-146) and to apply the mathematical relationship (section 5.3) to the prime number. One of ordinary skill in the art would have been motivated to do this because the mathematical relationship of Menezes is a one-way function and Menezes teaches that by selecting a prime

Art Unit: 2135

number for the values of p and q make the one-way function reverse of the function more difficult (Menezes Example 1.15 page 9 and section 5.14 page 174).

In reference to claims 2, 7, and 12, are rejected as in claim 1 above. However, in reference to determining at least one further subsequent prime number identification condition applied to a previously determined subsequent prime number, Menezes discloses combining the trial division stage and then the Miller-Rabin test (section 4.4.1). An in further reference to utilizing the mathematical relationship on a first subset of numbers selected from said set of numbers to generate a first random number, Menezes teaches using many sources and then sampling the sources (part ii of section 5.2 page 172).

In reference to claims 3 and 8, wherein said steps d through g are repeated to generate a desired number of idem-random numbers. Menezes teaches using many sources and then sampling the sources (part ii of section 5.2 page 172).

In reference to claims 4 and 9 Menezes discloses establishing desired distribution characteristics; determining a distribution operation to be applied to said idem-random (random number) numbers to create said desired distribution; and applying said distribution operation to said idem-random numbers to generate specifically distributed idem-random numbers (random number; pages 176-177).

In reference to claims 5 and 10 Menezes discloses establishing desired distribution characteristics; determining a distribution operation to be applied to said idem-random numbers (random number) to create said desired distribution; and applying said distribution operation to said idem-random numbers to generate specifically distributed idem-random numbers (pages 176-177).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

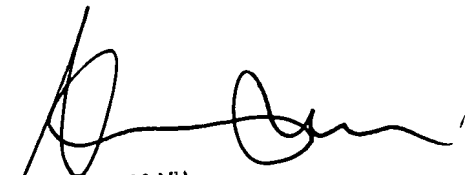
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PWK

Wednesday, November 07, 2007



KIM VU
SENIOR PATENT EXAMINER
TECHNICAL CENTER 2100